УДК 621.32

А. В. СИДОРЕНКО, И. В. ШАКИНКО

МОДИФИЦИРОВАННЫЙ МЕТОД ГЛАВНЫХ КОМПОНЕНТ ПРИ ШИФРОВАНИИ ИЗОБРАЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ ДИНАМИЧЕСКОГО ХАОСА

Исследованы выходные изображения алгоритмов шифрования при использовании модифицированного метода главных компонент.

Предлагается модификация метода главных компонент. Показано, что разработанный метод позволяет проанализировать количественно (по уровню вклада главных компонент) выходные изображения алгоритма шифрования на основе динамического хаоса.

Проведен сравнительный анализ результатов, полученных при использовании сингулярного спектрального анализа и модифицированного метода. Установлено, что модифицированный метод главных компонент, в отличие от сингулярного спектрального анализа, является чувствительным к форме гистограммы изображения.

Установлено, что стандартное отображение Чирикова и отображение пекаря являются подходящими для проведения процедуры «Перестановка пикселей» при шифровании изображений.

Ключевые слова: графическое представление матриц; динамический хаос; криптография; метод главных компонент; сингулярный спектральный анализ; уровень вклада главных компонент.

The given work is aimed at research of the output images of the algorithm based on deterministic chaos using the modified principal component analysis.

In this paper the modification of the principal component analysis is proposed. It has been found that the proposed method allows one to analyze quantitatively (by a level of the contribution made from the principal components) the output images of the encryption algorithm based on deterministic chaos.

The results obtained by the singular spectrum analysis and by the proposed method have been compared. It has been established that the modified principal component analysis, in contrast to the singular spectrum analysis, is sensitive to the shape of the image histogram.

It has been found that the Chirikov standard map and baker map are suitable for the procedure «Pixel permutation» when enciphering images.

Key words: cryptography; deterministic chaos; graphical matrix representation; principal component analysis; singular spectrum analysis.

Современные информационные технологии находят все более широкое применение в телекоммуникационных системах. Весьма актуальной становится задача разработки и внедрения надежных методов и средств защиты информации для обеспечения ее целостности и конфиденциальности.

Традиционные алгоритмы, такие как des, idea, aes, не являются подходящими для шифрования изображений. Вследствие большого размера шифруемых данных время на осуществление процедуры шифрования оказывается достаточно большим [1]. В качестве альтернативы для этих целей предлагается использовать алгоритмы на основе динамического хаоса. Для шифрования изображений используют схему, включающую в себя две независимые процедуры: «Перестановка пикселей» и «Диффузия». При проведении процедуры «Перестановка пикселей» происходит перестановка всех пикселей изображения согласно некоторому преобразованию. К преобразованию предъявляются следующие требования: возможность осуществления обратной перестановки пикселей для получения исходного изображения; перестановка должна осуществляться «непредсказуемым» образом.

В качестве преобразований, удовлетворяющих данным требованиям, в литературе предлагается использовать различные двумерные хаотические отображения. Однако вопрос о том, насколько хорошо конкретное двумерное хаотическое отображение скрывает структуру исходного изображения, не рассматривается.

Кроме того, в алгоритмах на основе динамического хаоса при функционировании необходимо обеспечение хаотического режима. Таким образом, требуется контроль степени хаотичности выходных последовательностей таких алгоритмов.

Ввиду того что выходные последовательности алгоритмов шифрования на основе динамического хаоса являются нестационарными, для их обработки возможно использование метода сингулярного спектрального анализа [2]. Но поскольку периодические процессы в рассматриваемых реализациях сами имеют нестационарности, то не всегда достаточно применение метода сингулярного спектрального анализа для выделения детерминированных составляющих [3]. В связи с этим возникает необходимость поиска других методов оценки хаотичности.

Модифицированный метод главных компонент

Для анализа информации, зашифрованной с использованием динамического хаоса, нами предложен метод, разработанный на базе метода главных компонент. Алгоритм модифицированного метода включает следующие этапы:

- тест на сгустки в системе итерированных функций;
- формирование распределения точек одной координатой;
- преобразование полученного распределения точек в матрицу;
- метод главных компонент.

Рассмотрим подробнее данные этапы.

1. Тест на сгустки в системе итерированных функций (IFS clumpiness test) [4]. Для определенности рассмотрим временной ряд A, содержащий N отсчетов:

$$A = \{a_1, a_2, ..., a_{N-1}, a_N\}. \quad (1)$$

Определяется диапазон принимаемых значений временного ряда в d:

$$d = a_{\max} - a_{\min}, \quad (2)$$

где $a_{\max}$ и $a_{\min}$ – максимальное и минимальное значения, принимаемые отсчетами временного ряда соответственно.

Полученный диапазон значений разбивается на 4 равных интервала:

$$\left[a_{\min}, a_{\min} + \frac{d}{4}\right); \quad (3)$$

$$\left[a_{\min} + \frac{d}{4}, a_{\min} + \frac{2d}{4}\right); \quad (4)$$

$$\left[a_{\min}+\frac{2d}{4}, a_{\min}+\frac{3d}{4}\right); \tag{5}$$

$$\left[a_{\min}+\frac{3d}{4}, a_{\max}\right]. \tag{6}$$

На плоскости чертится квадратное поле. Нумеруются углы, начиная с левого нижнего и далее двигаясь против часовой стрелки. Первой ставится точка по центру квадрата. Ставится новая точка посередине отрезка, соединяющего центральную точку и угол с номером, равным номеру интервала, которому принадлежит значение первого отсчета. Далее процедура повторяется для последующих отсчетов с отличием в том, что отрезок откладывается не от центральной, а от последней поставленной точки. Таким образом формируется распределение точек по квадрату.

2. Формирование распределения точек одной координатой.

Если ввести координатные оси $0X$ и $0Y$ вдоль двух перпендикулярных сторон квадрата, то каждой точке, принадлежащей квадрату, можно поставить в соответствие два числа: координату x и координату y. С учетом того, что каждому отсчету исходного временного ряда соответствует определенная точка, возможно сформировать набор пар значений «номер отсчета – координата точки». В качестве «координаты точки» выбираются либо координаты x, либо координаты y для всех пар. Каждую пару значений будем рассматривать как координаты некоторой точки, принадлежащей новому распределению точек по прямоугольной области B.

3. Преобразование полученного распределения точек в матрицу. Прямоугольная область B разбивается на $m \cdot n = R$ равных, не пересекающихся частей, где m – число делений области по горизонтали; n – по вертикали. Определим матрицу C, содержащую n строк и m столбцов, значения элементов которой определяются следующим образом:

$$c_{ij} = N_{ij}, \tag{7}$$

где N_{ij} – число точек, которые принадлежат ij-части области B, $i = 1, \ldots, n,\ j = 1, \ldots, m$.

4. К полученной матрице C применяется метод главных компонент, который включает следующие процедуры:

• центрирование и нормирование:

$$c^*_{ij} = \left(c_{ij} - \overline{c_j}\right) / s_j, \tag{8}$$

где $\overline{c_j} = \left(\sum_{i=1}^{n} c_{ij}\right) / n,\ s_j = \sqrt{\left(\sum_{i=1}^{n}\left(c_{ij} - \overline{c_j}\right)^2\right)} / n,\ i = 1, \ldots, n, j = 1, \ldots, m;$

• разложение по сингулярным значениям (SVD):

$$C^* = USV^t; \tag{9}$$

• вычисление матрицы счетов:

$$T = US; \tag{10}$$

• вычисление собственных значений:

$$L = T^t T; \tag{11}$$

• нормировка каждого собственного значения на сумму всех собственных значений (определение уровня вклада каждой компоненты):

$$\lambda_i = l_i / \sum_{j=1}^{k} l_j, \tag{12}$$

где $k = \min(n, m),\ i = 1, \ldots, k$.

Следует отметить, что чем выше уровень вклада первой главной компоненты, тем выше вклад детерминированных составляющих в рассматриваемую реализацию.

Результаты исследования и их обсуждение

Обработке подвергались два изображения размером 128 на 128 пикселей: «Lena.bmp» и «Chessboard.bmp». Изображение «Chessboard.bmp» было сформировано таким образом, что количество пикселей с равными значениями яркости равнялось 64.

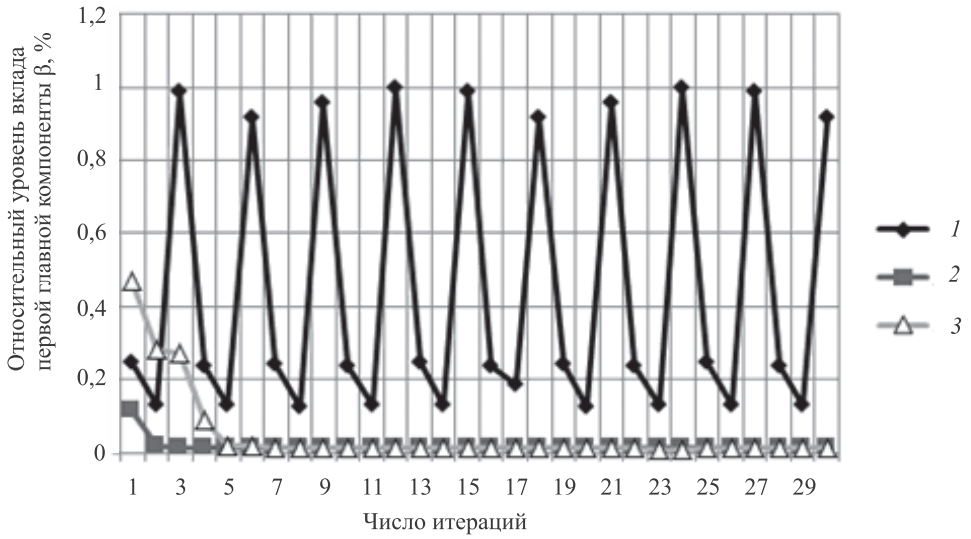

Рис. 1. График зависимости относительного уровня вклада первой главной компоненты от числа итераций для изображения «Chessboard.bmp» при использовании модифицированного метода главных компонент: *1* – двумерное хаотическое отображение «кот Арнольда»; *2* – стандартное отображение Чирикова; *3* – отображение пекаря

При моделировании использовались три двумерных хаотических отображения в процессе проведения процедуры «Перестановка пикселей»: «кот Арнольда», отображение пекаря и стандартное отображение Чирикова. Число итераций хаотических отображений менялось от 1 до 30. Размеры формируемых матриц при использовании модифицированного метода главных компонент выбирались равными: $n = 900$ и $m = 900$.

Для визуального представления полученных данных были построены графики зависимости относительного уровня вклада первой главной компоненты от числа итераций хаотического отображения. При использовании двумерного хаотического отображения «кот Арнольда» для изображения «Chessboard.bmp» наблюдается периодичность максимумов и минимумов в значениях уровней вклада первой главной компоненты в зависимости от числа итераций (рис. 1). Однако даже при минимальных значениях данного показателя его численное значение составляет примерно 0,15. В случае изображения «Lena.bmp» периодичность не наблюдается, значение относительного уровня вклада первой главной компоненты, как и в предыдущем случае, не меньше 0,15 (рис. 2). В то же время для некоторых итераций значение данной величины достигает 0,4. Для двумерных хаотических отображений – отображения пекаря и стандартного отображения Чирикова – относительный уровень вклада первой главной компоненты при увеличении числа итераций уменьшается. Однако при использовании стандартного отображения Чирикова относительный уровень вклада первой главной компоненты спадает быстрее по сравнению с отображением пекаря и достигает минимальных значений уже на третьей итерации. Стоит отметить, что минимальные значения, полученные при использовании данных двух хаотических отображений, применяемых для изображения «Lena.bmp» и «Chessboard.bmp», составляют 0,2 и 0,012 соответственно и отличаются более чем в 10 раз. Таким образом, модифицированный метод является чувствительным к форме гистограммы обрабатываемых изображений.

Рассматриваемые реализации были также обработаны с использованием варианта сингулярного спектрального анализа, предназначенного для обработки двумерных полей (рис. 3). Значения относительного уровня вклада первой главной компоненты, полученные при использовании отображения пекаря и стандартного отображения Чирикова для изображений «Lena.bmp» и «Chessboard.bmp» при числе итераций, большем 18, примерно совпадают и находятся в пределах от 0,01 до 0,015. Таким образом, применение сингулярного спектрального анализа не выявляет различия между изображениями с разной формой гистограммы.

В результате проведенных исследований показано, что модифицированный метод главных компонент позволяет проанализировать количественно (по уровню вклада главных компонент) выходные последовательности алгоритма шифрования на основе динамического хаоса.

Установлено, что модифицированный метод главных компонент, в отличие от сингулярного спектрального анализа, является чувствительным к форме гистограммы изображения при проведении процедуры «Перестановка пикселей».

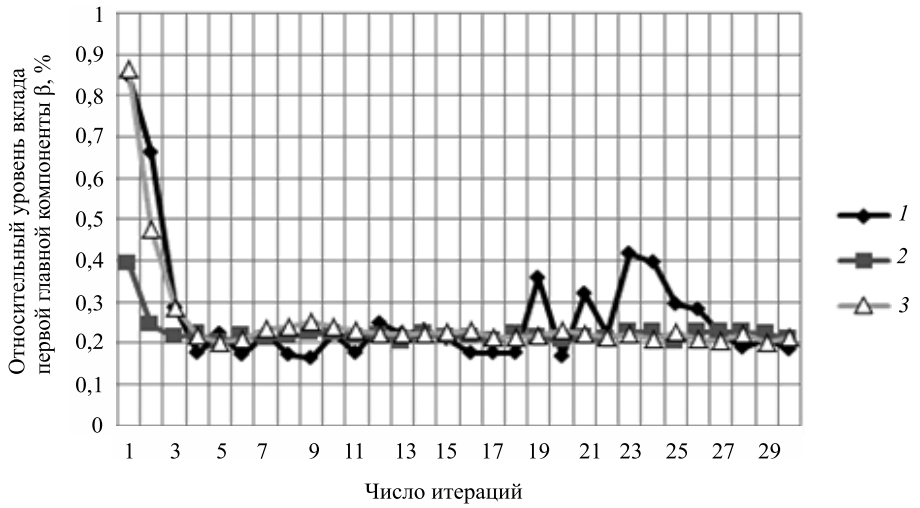

Рис. 2. График зависимости относительного уровня вклада первой главной компоненты от числа итераций для изображения «Lena.bmp» при использовании модифицированного метода главных компонент:
1 – двумерное хаотическое отображение «кот Арнольда»; *2* – стандартное отображение Чирикова; *3* – отображение пекаря

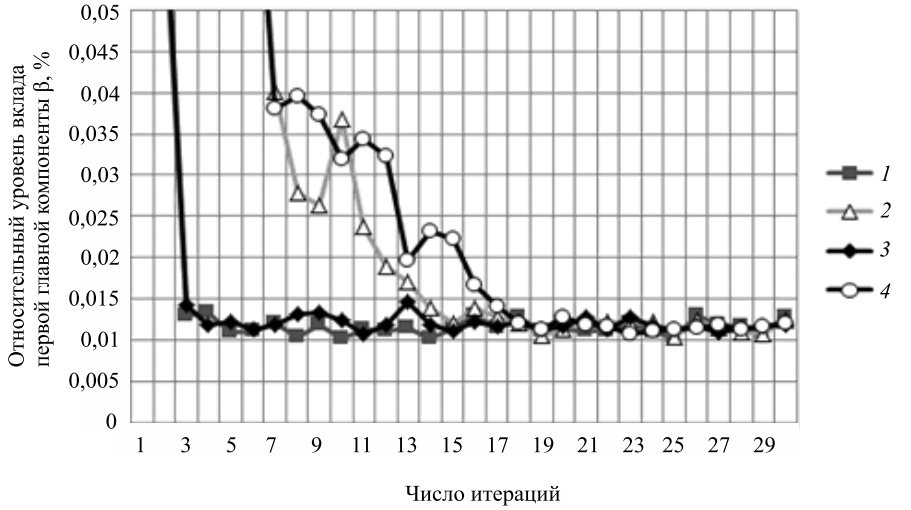

Рис. 3. График зависимости относительного уровня вклада первой главной компоненты от числа итераций при использовании сингулярного спектрального анализа:
1 – стандартное отображение Чирикова (изображение «Chessboard.bmp»); *2* – отображение пекаря (изображение «Chessboard.bmp»); *3* – стандартное отображение Чирикова (изображение «Lena.bmp»); *4* – отображение пекаря (изображение «Lena.bmp»)

На основании результатов расчета уровня вклада главных компонент установлено, что для проведения процедуры «Перестановка пикселей» при шифровании изображений подходящими являются стандартное отображение Чирикова и отображение пекаря в отличие от отображения «кот Арнольда», при использовании которого полученные изображения обладают высокой структурированностью.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Ye G. A block image encryption based on wave transmission and chaotic systems // Nonlinear Dynamics. 2014. Vol. 75, № 3. P. 417–427.

2. Сидоренко А. В., Шакинко И. В. Шифрование на основе динамического хаоса с использованием сингулярного спектрального анализа : сб. работ 69-й науч. конф. студентов и аспирантов БГУ : в 3 ч. (Минск, 14–17 мая 2012 г.). Минск, 2012. Ч. 1. С. 276–279.

3. Борог В. В., Крянев А. В., Удумян Д. К. Комбинированный метод выявления скрытых аномалий в хаотических временных процессах // Фундаментальные физико-математические проблемы и моделирование технико-технологических систем : сб. науч. тр. 2009. Вып. 12. С. 536–546.

4. Меклер А. А. Применение аппарата нелинейного анализа динамических систем для обработки сигналов ЭЭГ // Актуальные проблемы современной математики : ученые зап. 2004. Вып. 2. С. 112–140.

Поступила в редакцию 19.06.2014.

Алла Васильевна Сидоренко – доктор технических наук, профессор кафедры физики и аэрокосмических технологий.

Иван Владимирович Шакинко – магистрант факультета радиофизики и компьютерных технологий. Научный руководитель – А. В. Сидоренко.